웹 통신 구조로 이해하는 OSI 7계층과 TCP/IP 네트워크 실무

1. 네트워크 모델의 기본 개념

1-1. 네트워크(Network)

서로 다른 컴퓨터나 장치(PC, 서버, 스마트폰 등)가 **데이터를 주고받기 위해 연결된 구조**입니다.
이 연결은 단순한 케이블 연결이 아니라, **약속된 규칙(Protocol, 프로토콜)**을 지켜야만 가능합니다.

1-2. 프로토콜 (Protocol)

네트워크에서 장치끼리 통신하기 위한 **규칙, 절차, 형식**을 의미합니다.
즉, "데이터를 어떤 순서로, 어떤 형식으로, 언제 보낼 것인가"에 대한 국제적인 약속입니다.

예:

- 사람 간 대화에서 '말할 때 한 명씩 말하고, 인사 후 대화 시작한다'는 규칙과 유사.
- 네트워크에서는 이를 기계적으로 수행하기 위해 프로토콜을 사용.

1-3. 계층(Layer)의 개념

네트워크 통신은 매우 복잡합니다.
그래서 이를 단계별(층, Layer)로 나누어 이해하기 쉽게 만든 것이 "계층 모델"입니다.

- **상위계층**: 사용자가 직접 다루는 영역 (응용, 표현, 세션 등).
- **하위계층**: 실제 물리적 데이터 전송을 담당 (전송, 네트워크, 데이터링크, 물리 등).

1-4. OSI vs TCP/IP

구분	OSI 7계층	TCP/IP 4계층
목적	통신 구조를 설명하는 이론적 모델	실제 인터넷 통신에서 사용하는 실무 모델
관리기관	ISO (국제표준화기구)	IETF (인터넷기술표준기구)
구조	7단계로 세분화	4단계로 단순화
사용	교육, 이론, 설계표준	실제 네트워크 장비 및 운영체제에서 사용

2. OSI 7계층 개요

2-1. OSI 모델이란?

OSI(Open Systems Interconnection) 모델은 국제표준화기구 ISO가 제정한 **컴퓨터 간 통신 표준 구조**입니다.
복잡한 네트워크 통신을 7단계로 나누어 각 단계가 담당하는 역할을 명확히 했습니다.

OSI 계층	한글명	영문명	핵심 역할(요지)
7	응용	Application	사용자/앱이 직접 쓰는 네트워크 서비스 제공
6	표현	Presentation	데이터 인코딩·압축·암호화(형식 변환)
5	세션	Session	연결(Session) 생성·유지·복구
4	전송	Transport	종단 간 신뢰성·포트 관리(TCP/UDP)
3	네트워크	Network	IP 주소 기반 라우팅(경로 선택)
2	데이터링크	Data Link	같은 네트워크 내 프레임 전송(MAC)
1	물리	Physical	전기/광 신호로 실제 전송(비트)

2-2. 목적

- 서로 다른 시스템과 운영체제 사이에서도 통신 가능하게 표준화.
- 문제 발생 시 "어느 계층"에서 문제인지 쉽게 진단.
- 각 계층이 독립되어 있어 하나를 바꾸어도 전체 영향 최소화.

2-3. 데이터 단위 (PDU)

OSI 계층	데이터 단위(PDU)	설명
7 ~ 5	**Data**	사용자 데이터
4	**Segment**	TCP 또는 UDP 단위
3	**Packet**	IP 주소 기반 데이터 묶음
2	**Frame**	MAC 주소 기반 전송 단위
1	**Bit**	전기·광 신호 0,1

2-4. 상위계층 vs 하위계층 (캡슐화 / 역캡슐화)

송신측: 7 → 1 (데이터에 헤더 추가).

수신측: 1 → 7 (헤더 제거 및 복원).

- **캡슐화(Encapsulation)**: 데이터에 계층별 정보를 덧붙이는 것.
- **역캡슐화(Decapsulation)**: 받는 쪽이 그 정보를 벗겨내는 것.

예: 웹브라우저가 HTTP 요청을 보내면 → TCP 세그먼트로 감싸고 → IP 패킷으로 포장 → 이더넷 프레임으로 보내며, 반대로 서버는 이 포장을 한 겹씩 풀어 원본 요청을 읽습니다.

3. 각 계층별 상세 설명 (1 ~ 7계층)

3-1. 1계층 – 물리 (Physical Layer)

- 전기·광학 신호를 이용해 0과 1비트로 데이터를 보냄.
- 하드웨어 규격(RS-232, Wi-Fi, 광케이블 등) 정의.
- 실제 '전송선로' 역할.

예: LAN 케이블 – 전류 높으면 1, 낮으면 0으로 표현.

3-2. 2계층 – 데이터링크 (Data Link Layer)

- **같은 네트워크(LAN)** 내에서 프레임(Frame) 전송.
- **MAC 주소**로 기기 식별.
- 오류 검출(FCS), 흐름제어 수행.

프로토콜: Ethernet, PPP, VLAN(802.1Q), ARP
장비: 스위치(Switch)

3-3. 3계층 – 네트워크 (Network Layer)

- **IP 주소** 기반으로 경로 선택 및 라우팅.
- 패킷(Packet) 단위 전송.
- 서로 다른 네트워크 간 데이터 전달.

프로토콜: IP, ICMP(ping), BGP, OSPF
장비: 라우터(Router), L3 스위치

※ OSPF는 IP 프로토콜 위에서 작동하며, BGP는 TCP(4계층) 위에서 작동함.

3-4. 4계층 – 전송 (Transport Layer)

- "프로그램 간 통신"을 책임지는 계층.
- **포트 번호(Port)** 로 애플리케이션 식별.
- 데이터의 신뢰성과 속도를 관리.

3-4-1. TCP (Transmission Control Protocol)

항목	설명
정의	신뢰성 있는 연결형(Connection-Oriented) 프로토콜
연결 방식	3-Way Handshake (SYN→SYN+ACK→ACK)
특징	순서 보장, 재전송, 흐름제어(Window Control), 혼잡제어
단위	세그먼트(Segment)
장점	정확성 보장, 데이터 손실 복구
단점	속도 느림, 오버헤드 큼
예시	HTTP, HTTPS, FTP, SMTP, SSH

※ 3-Way Handshake 절차

1) Client → SYN → Server

2) Server → SYN+ACK → Client

3) Client → ACK → Server

연결 종료는 4-Way Handshake(FIN→ACK→FIN→ACK).

3-4-2. UDP (User Datagram Protocol)

항목	설명
정의	비연결형(Connectionless), 빠른 전송 프로토콜
특징	순서 보장 없음, 재전송 없음, 헤더 8 바이트로 가벼움

장점	속도 빠름, 지연 적음
단점	신뢰성 낮음
예시	DNS, DHCP, 게임, 스트리밍, VoIP

3-4-3. TCP vs UDP 비교

항목	**TCP**	**UDP**
연결 방식	연결형	비연결형
신뢰성	높음	낮음
속도	느림	빠름
순서 보장	O	X
재전송	O	X
대표 서비스	웹, 메일	스트리밍, 게임, IoT

3-5. 5계층 – 세션 (Session Layer)

- 연결(Session)의 설정·유지·복구.
- 예: FTP 연결 유지, RTSP 영상 제어.

3-6. 6계층 – 표현 (Presentation Layer)

- 데이터 형식 변환 및 암호화.
- 예: HTTPS의 TLS 암호화, 문자 코드 변환(ASCII ↔ Unicode).

3-7. 7계층 – 응용 (Application Layer)

- 사용자 직접 접근 계층.
- 실제 서비스 제공.

예: HTTP(웹), FTP(파일), SMTP/IMAP(메일), SSH(원격), DNS(이름해석), MQTT(IoT).

3-8. OSI 7계층 요약

OSI 계층	주요 기능	데이터 단위	대표 프로토콜 / 기술	대표 장비	실제 사례(웹 포함)
1	전기/광 신호 전송(0/1)	Bit	UTP, 광(Optical Fiber), RS-232(직렬), 802.11(Wi-Fi)	케이블, 허브, 무선AP	케이블 길이/품질, 전압/레이저로 신호 전송
2	같은 LAN에서 **MAC** 기반 프레임 전달, 오류검출(FCS)	Frame	Ethernet(이더넷), ARP(IP↔MAC), VLAN(802.1Q)	스위치	스위치가 MAC 학습 후 해당 포트로만 전달
3	IP 주소로 라우팅(경로 선택), 서로 다른 네트워크 연결	Packet	IP(v4/v6), ICMP(핑), OSPF/BGP(라우팅)	라우터, L3 스위치	사무실→인터넷 경로 계산, 핑 테스트
4	종단 간 통신, 포트 관리, 신뢰성/속도	Segment	TCP(신뢰성), UDP(속도), QUIC	L4 스위치(로드 밸런서)	HTTP=TCP 80/443, DNS=UDP 53
5	연결 생성·유지·동기화	Data	NetBIOS, RPC, RTSP	–	FTP 연결 유지, 스트리밍 제어
6	암호화·압축·인코딩	Data	TLS 1.2+(HTTPS 암호화), ASCII/Unicode, JPEG/MPEG	–	HTTPS에서 TLS 핸드셰이크·암호화
7	사용자 서비스/프로토콜	Data	HTTP/HTTPS, FTP, SMTP/IMAP/POP3, DNS, SSH, MQTT/CoAP	PC/서버	브라우저로 웹 열기, 메일 송수신

4. 네트워크 장비와 계층 관계

4-1. 장비 역할 비교

장비	해당 OSI 계층	핵심 역할	비고
허브(Hub)	1	신호 단순 복제/중계(모든 포트로 뿌림)	충돌 많아 현대엔 거의 미사용

스위치 (Switch)	2	MAC 주소 테이블로 목적 포트만 전송	기본적으로 하나의 브로드캐스트 도메인, VLAN을 통해 브로드캐스트 도메인 분리 가능
라우터 (Router)	3	IP 라우팅(서로 다른 네트워크 연결)	게이트웨이 역할
L3 스위치	2~3	스위칭 + VLAN 간 라우팅 (SVI)	하드웨어 라우팅으로 고속
L4 스위치	4	포트/세션 기반 **로드밸런서**	다수 서버로 트래픽 분산

4-2. 스위치 포트 구조 및 VLAN 관계

- **Access 포트**: 단일 VLAN(비태그, untagged)로 단말 접속.
- **Trunk 포트**: 다중 VLAN(태그, tagged) 묶어서 스위치↔스위치/라우터로 운반.
- **Hybrid 포트**: Access+Trunk 혼합(단말+AP/서버에 유용).

4-3. 라우터·스위치 다중 연결 (1:N, N:1)

- **스위치 1 ↔ 라우터 여러 대(N:1의 반대)**: 다중 회선/망 분리/이중화(예: KT+SKB+전용망).
- **라우터 1 ↔ 스위치 여러 대(1:N)**: 사무실/층별로 스위치 확장.
- **L3 스위치**: 여러 라우터 기능을 **SVI(Switched Virtual Interface)** 로 통합.

4-4. 장비에서의 계층 상승(1→2→3 처리)

- 스위치는 **2계층**까지만 해석(MAC까지).
- 라우터는 **3계층**까지 해석(IP까지) 후 다음 홉(**hop**: 패킷이 지나가는 **라우터 한 대**를 1홉이라고 부름)으로 전달.
- 각 장비는 **자신의 최대 계층까지만** 내용을 보고 다시 하위 신호로 변환해 보냄.

5. VLAN (가상 랜, Virtual LAN)

5-1. 정의

물리적으로 하나의 스위치를 **논리적으로 여러 네트워크**로 나누는 기술.
브로드캐스트 범위를 분리하여 보안·성능 향상.

5-2. 동작 원리(802.1Q 태깅)

- 프레임에 **VLAN ID(12비트)** 태그를 붙여 구분(0~4095 중 1~4094 사용, 0=우선순위 태그(PRI용), 4095=예약(Reserved)).
- 같은 VLAN끼리만 2계층 통신 가능.

5-3. 포트 구분

유형	특징	용례
Access	1개 VLAN만 수용(무태그)	PC/프린터 등 단말
Trunk	다수 VLAN 태깅 전달	스위치↔스위치, 스위치↔라우터
Hybrid	혼합 운용	AP/서버 등

5-4. VLAN 간 통신(Inter-VLAN Routing)

- **라우터 온 어 스틱(Router-on-a-Stick)**: 라우터 한 포트에 VLAN별 서브인터페이스로 라우팅.
- **L3 스위치 SVI**: VLAN 인터페이스에 IP를 주고 내부에서 고속 라우팅.

5-5. 보안·실무 팁

- **DHCP 스누핑(DHCP Snooping)**으로 비인가 DHCP 차단.
- **DAI(Dynamic ARP Inspection)**로 ARP 위조 방지.
- **네이티브 VLAN** 설정 일관성 유지(Trunk 양단 동일).

6. 라우터-스위치 연결 구조 비교

구조	목적	장점	단점	실무 예
스위치 1 + 라우터 여러 대	다중망·이중화·망 분리	장애 대비, 정책 라우팅	구성 복잡	기관망+인터넷망+게스트망
라우터 1 + 스위치 여러 대	내부망 확장	단순, 표준적	단일 게이트웨이 의존	사무실/캠퍼스 기본
L3 스위치 단독	통합	고속 라우팅, 관리 단순	장비 단가	데이터센터·코어망

7. 인터넷 회선과 OSI 계층 관계

7-1. "회선"은 1~3계층의 결합

- **1계층**: 광/동선로, 전파(물리 전송).
- **2계층**: PPPoE(포인트 투 포인트 프로토콜 over 이더넷), 이더넷 프레이밍.
- **3계층**: IP 라우팅(통신사 코어망의 **BGP** 등).

7-2. ISP(Internet Service Provider) 내부 라우팅

- 엣지→코어 라우터를 거치며 **OSPF(내부)**, **BGP(외부)** 로 경로 학습.
- 고객 트래픽은 ISP의 **자율시스템(AS, Autonomous System)**을 지나 목적지 AS로 전달.

8. NIC(네트워크 인터페이스 카드, Network Interface Card)와 다중망

8-1. NIC 기본

- OSI **1~2계층**을 담당하는 **네트워크 카드**.
- 고유 **MAC 주소** 보유, 링크 속도/듀플렉스 협상(오토 네고시에이션).

8-2. NIC 2개 장착(듀얼 NIC)으로 2개 망 동시에 사용

```
PC
├── NIC1 → 스위치/VLAN A → 라우터 A(사내망)
└── NIC2 → 스위치/VLAN B → 라우터 B(인터넷/별도망)
```

- **OS 라우팅 테이블**이 목적지 IP에 따라 어떤 NIC/게이트웨이를 사용할지 자동 결정.
- **기본 경로(Default Route)**는 보통 1개 NIC에만 부여(중복 시 충돌). 단, OS별로 Metric 우선순위를 통해 다중 기본 게이트웨이 동작이 가능함.
- **DNS** 도 망별로 분리 설정하면 혼선 감소.

8-3. 브라우저 동작 원리(주소→DNS→라우팅→NIC 선택)

1. 사용자가 URL 입력 →
2. **DNS(도메인 네임 시스템, Domain Name System)** 로 IP 조회(보통 **UDP 53** 포트) →
3. OS가 **라우팅 테이블**로 경로 결정(목적지 IP가 내부면 NIC1, 외부면 NIC2 등) →

4. 선택된 NIC로 **TCP/UDP** 송신 →
5. 라우터를 통해 목적지로 전송.

8-4. 단일 NIC / 듀얼 NIC / VLAN / 정책 라우팅 비교

방식	개요	장점	단점	용례
단일 NIC	하나의 인터페이스	단순	다중망 동시 사용 불가	일반 PC
듀얼 NIC	물리 NIC 2개	두 망 동시 사용	라우팅·DNS 관리 필요	망 분리 PC, 서버
VLAN NIC	하나의 물리 NIC 위에 **VLAN 태그 인터페이스** 여러 개	케이블 1개로 다중망	OS·스위치 설정 필요	서버/가상화
정책 라우팅 (PBR)	트래픽 조건별 다른 게이트웨이	유연	고급 설정	데이터센터·보안망

9. HTTP 외 다양한 네트워크 프로토콜

9-1. OSI 7계층별 주요 프로토콜(대표 포트 포함)

OSI 계층	프로토콜	기본 포트	설명/용도
7	**HTTP**	80	웹
7	**HTTPS**	443	암호화된 웹
7	**FTP(File Transfer Protocol)**	21(제어), 20(데이터)	파일 전송
7	**SMTP(Simple Mail Transfer Protocol)**	25(587/Submission)	메일 송신
7	**IMAP/POP3**	143/110 (TLS: 993/995)	메일 수신
7	**DNS(Domain Name System)**	53(UDP/TCP)	도메인→IP 해석
7	**SSH(Secure Shell)**	22	원격 접속(암호화)
7	**SNMP(Simple Network Management Protocol)**	161/162	장비 모니터링

7	**MQTT(Message Queuing Telemetry Transport)**	1883(8883/TLS)	IoT 경량 메시징
7	**CoAP(Constrained Application Protocol)**	UDP 기반	IoT용 경량 웹 유사
6	**TLS 1.2+**	–	암호화/인증(HTTPS, SMTPS 등)
5	**RTSP(Real Time Streaming Protocol)**	554	스트리밍 제어
4	**TCP/UDP/QUIC**	–	종단 통신/속도·신뢰성 선택
3	**IP/ICMP/IGMP/BGP/OSPF**	–	라우팅/진단/멀티캐스트
2	**Ethernet/VLAN/ARP**	–	프레임 전송/주소 변환
1	**802.11, RS-232, Fiber**	–	무선/직렬/광 물리 신호

9-2. 5~7계층 통합 구조(응용 영역)

현대 운영체제/스택은 **세션(5)·표현(6)·응용(7)** 을 통합 구현("Application Layer").
예: **HTTPS = HTTP(7) + TLS(6) + (세션 유지 기능 일부 포함).**

9-3. 프로토콜 상세 비교

- **HTTP vs HTTPS**: 후자는 **TLS** 로 암호화/서버 인증.
- **FTP vs SFTP(Secure FTP)**: SFTP는 **SSH(보안 채널)** 사용.
- **DNS(UDP)**: 기본 UDP 53 사용, 응답 크기 512바이트 초과 시 **TCP 53**으로 전환 (존 전송, DNSSEC 등).
- **MQTT vs CoAP**: MQTT는 TCP 기반 브로커 모델, CoAP는 UDP 기반 경량 REST 유사.

10. 전체 통신 흐름 통합 시나리오 ("PC → 스위치 → 라우터 → 인터넷 회선 → 서버")

10-1. 전송 시(클라이언트 → 서버)

1. **응용(7)**: 브라우저가 GET /search?q=test 생성(HTTP/HTTPS).
2. **표현(6)**: HTTPS라면 **TLS**로 암호화·인증.
3. **세션(5)**: 연결 유지·복구 상태 관리.
4. **전송(4)**: **TCP**가 3-Way Handshake 후 세그먼트 전송(또는 **UDP** 즉시 전송).
5. **네트워크(3)**: **IP**가 목적지 주소로 라우팅(경로 선택).
6. **데이터링크(2)**: **MAC** 목적지로 프레임화(스위치가 포워딩).
7. **물리(1)**: 비트 신호로 케이블/무선 통해 송출.

10-2. 중간 장비 처리

- **스위치(2)**: 프레임의 **MAC** 만 보고 올바른 포트로 전달.
- **라우터(3)**: **IP**를 보고 다음 홉/인터넷으로 라우팅(필요 시 **NAT**).
- **ISP 회선(1~3)**: 통신사 코어망을 BGP/OSPF로 경유.

10-3. 수신 시(서버 측 1→7 역캡슐화)

1. 물리 신호 수신 →
2. 프레임 해석(MAC) →
3. 패킷 해석(IP, 라우팅 도착 확인) →
4. 세그먼트 재조립(TCP 순서/재전송) →
5. 세션/표현(복호화) →
6. 응용(요청 처리, 응답 생성).

응답은 같은 경로를 반대로 따라 돌아옵니다.

11. TCP/IP 4계층과 OSI 7계층 대응

11-1. TCP/IP 4계층(실제 구현 모델)

TCP/IP 계층	한글명	영문명	역할	OSI 계층 대응	대표 프로토콜
4	응용	Application	사용자 서비스 (5~7 통합)	7·6·5	HTTP, TLS, FTP, DNS, SSH, MQTT

3	전송	Transport	포트·신뢰성/속도	4	TCP, UDP, QUIC
2	인터넷	Internet	IP 라우팅	3	IP, ICMP, OSPF, BGP
1	네트워크 접근	Network Access	프레임·물리 신호	2·1	Ethernet, Wi-Fi, VLAN, PPP, ARP

11-2. OSI 7계층 ↔ TCP/IP 4계층 대응표(주요 프로토콜 위치도)

OSI 계층	TCP/IP 계층	주요 프로토콜/기술	비고
7	4	HTTP/HTTPS, FTP, SMTP/IMAP/POP3, DNS, SSH, SNMP, MQTT/CoAP	사용자 서비스
6	4 통합)	TLS 1.2+, JPEG, ASCII/Unicode	암호화/인코딩
5	4(통합)	RTSP, RPC, SOCKS	연결 관리
4	3	TCP, UDP, QUIC	포트/신뢰성
3	2	IP, ICMP, IGMP, OSPF, BGP	라우팅/주소
2	1	Ethernet, VLAN(802.1Q), LACP, PPP, ARP	프레임/링크
1	1(통합)	UTP, Fiber, 802.11(Wi-Fi), RS-232	신호 매체

12. 마무리 정리

- **OSI 7계층**은 통신의 **개념 지도**, **TCP/IP 4계층**은 그 지도를 따라 지어진 **실제 도로망**입니다.
- **TCP**는 "정확히 보내기(신뢰성)", **UDP**는 "빨리 보내기(지연 최소)"를 목표로 합니다.
- **스위치(2계층)**는 LAN 내부를, **라우터(3계층)**는 네트워크간 길 찾기를 담당합니다.
- **VLAN**은 하나의 스위치를 여러 **논리 네트워크**로 나누며, **L3 스위치**가 VLAN간 라우팅을 통합합니다.
- **NIC 다중화**와 **OS 라우팅 테이블** 덕분에 한 PC가 **둘 이상의 망**을 동시에 안전하게 사용할 수 있습니다.
- 실제 웹 통신은 "**응용→전송→네트워크→데이터링크→물리**"로 포장되어 이동하고, 서버에서는 그 역순으로 풀려 처리됩니다.

13. 웹 개발 디버깅과 OSI 7계층 사례

13-1. 개요

웹 애플리케이션 개발 과정에서 오류나 지연이 발생할 때, 개발자는 **브라우저 개발자 도구 (Chrome DevTools)** 의 **Network 탭**을 활용하여 요청과 응답의 흐름을 분석합니다.
이 분석 과정은 실제 OSI 7계층 및 TCP/IP 4계층이 어떻게 동작하는지를 직접적으로 확인할 수 있는 대표적인 실무 사례입니다.

13-2. 상황 예시

프론트엔드 개발 중 API 호출이 실패(예: 404 Not Found, 500 Internal Server Error)한 경우, 개발자는 다음 절차를 통해 문제를 분석합니다.

1. 크롬 브라우저에서 F12 또는 Ctrl + Shift + I 로 **개발자 도구** 실행.
2. **Network 탭** 선택 후 요청(Request) 및 응답(Response) 상세 확인.
3. 요청 헤더, 응답 코드, 전송 시간 등을 단계별 점검.

이 과정에서 실제로 OSI 7계층의 흐름이 순서대로 일어납니다.

13-3. 계층별 동작 및 관찰 포인트

OSI 계층	핵심 역할	Chrome DevTools 또는 OS에서 확인 가능한 항목
7	브라우저가 HTTP/HTTPS 요청 생성 및 응답 수신	Headers 탭의 Request URL, Method, Status Code, Content-Type
6	데이터 인코딩·압축·암호화 (예: JSON, GZIP, TLS)	Response 탭의 application/json, Content-Encoding: gzip, Provisional headers
5	연결 유지 및 인증·세션 상태 관리	Headers의 Connection: keep-alive, Cookie, Authorization
4	TCP 연결 수립(3-Way Handshake), 포트 관리	Timing 탭의 Connecting, SSL Handshake, TTFB(Time to First Byte)
3	IP 주소 기반 라우팅, DNS 질의 처리	Headers의 Remote Address, DNS Lookup 구간 시간
2	MAC 주소 기반 프레임 전송 (LAN 내부 통신)	OS 명령(arp -a)로 MAC 확인 가능
1	실제 케이블/무선 신호를 통한 전송	LAN 케이블, Wi-Fi 연결, NIC 상태

13-4. TCP/IP 4계층과의 연계

TCP/IP 계층	OSI 계층 대응	실제 웹 디버깅 대응 항목
4	OSI 5~7	HTTP/HTTPS 요청, 헤더, 쿠키, JSON 응답
3	OSI 4	TCP 연결, 재전송, 패킷 손실, RTT 측정
2	OSI 3	IP, DNS, 라우팅, NAT 확인
1	OSI 1~2	이더넷, Wi-Fi, NIC 설정, 링크 상태

13-5. 실제 개발 사례별 계층 분석

증상	관찰 지점	해당 OSI 계층	분석 결과 예시
404 Not Found	Network 탭 Status Code	7	서버 라우팅 미등록, 엔드포인트 오류
500 Internal Server Error	Response Body, Headers	7	서버 내부 예외 발생
요청 지연 (TTFB 길음)	Timing 탭 Waiting (TTFB)	4	TCP 재전송, 혼잡제어, 네트워크 지연
ERR_CERT_AUTHORITY_INVALID	브라우저 경고창	6	TLS 인증서 문제
ERR_NAME_NOT_RESOLVED	Network 탭 미출력	3	DNS 해석 실패
로컬 서버 연결 불가	Wi-Fi/유선 연결 끊김	1	물리계층 장애 (케이블, 무선 연결 문제)

13-6. 개발자 관점 요약

- 크롬의 **Network 탭은 OSI 7계층의 동작을 시각화한 도구**로 볼 수 있다.
- 단순히 "API 호출 실패"가 아니라, **어느 계층에서 문제 발생했는지** 구분 가능하다.
- 예:
    - 코드(응용계층) 문제 → API 엔드포인트 수정.
    - 전송 지연(전송계층) → 네트워크 지연/재전송 분석.
    - 인증서 오류(표현계층) → TLS 설정 점검.

13-7. 결론

웹 개발자는 코드뿐 아니라 네트워크 전 계층을 이해해야 문제를 정확히 진단할 수 있습니다.
OSI 7계층은 이론, **Chrome Network 탭은 실무의 창**으로, 양자를 연결하면 개발 효율과 문제 해결 능력을 함께 높일 수 있습니다.

13-8. 실제 웹 개발 적용 사례

13-8-1. API 연동 및 네트워크 요청 분석

상황:
React 또는 Next.js 기반 프론트엔드에서 axios 또는 fetch로 백엔드 API 호출 시, CORS 오류, 응답지연, 인증 실패 등의 문제 발생.

문제 유형	확인 위치	해당 OSI 계층	설명 및 해결방안
CORS 정책 오류 (Access-Control-Allow-Origin)	Network → Headers	7	서버 응답 헤더 미설정 → 백엔드에서 CORS 미들웨어 추가 (app.enableCors())
응답 지연	Network → Timing → Waiting (TTFB)	4	TCP 세그먼트 재전송 또는 서버 처리 지연 → 백엔드 성능 분석 필요
인증 토큰 만료	Headers → Authorization	5	JWT 또는 세션쿠키 갱신 필요
데이터 포맷 오류 (Unexpected token < in JSON)	Response 탭	6	서버에서 HTML 오류페이지 반환 → Content-Type 미일치
API Endpoint 오타	Request URL	7	/api/userinfo → /api/users/info 등 엔드포인트 불일치

13-8-2. 로그인 / 인증 흐름 분석 (HTTPS + JWT 기반)

상황:
로그인 시 HTTPS 통신과 JWT 토큰이 함께 동작함. 이때 계층별 역할을 명확히 구분할 수 있다.

OSI 계층	역할 및 관련 기술	실제 확인 항목
7	REST API 요청 (POST /auth/login) / 응	Request URL, Status Code

	답 (200 OK)	
6	HTTPS(TLS) 암호화 / JSON 포맷 응답	Content-Type: application/json, secure 표시
5	JWT 토큰을 통한 인증 세션 유지	Headers의 Authorization: Bearer
4	TCP 443 포트 연결, 신뢰성 있는 데이터 전송	Timing 탭의 SSL handshake, Waiting
3	IP 주소 라우팅 (내부망 → 외부망)	Remote Address, DNS Lookup
1~2	NIC, Wi-Fi 연결 품질	OS 네트워크 아이콘, ping 응답속도

→ **분석 포인트:** 로그인 실패 시 "토큰 누락"이면 응용계층 문제, "HTTPS 인증서 오류"면 표현계층 문제임을 구분 가능.

13-8-3. 이미지 업로드 및 S3 Presigned URL 전송

상황:
사용자가 웹에서 이미지를 업로드할 때, S3와 같은 Object Storage로 Presigned URL을 통해 직접 업로드하는 구조. 이때 **대용량 파일 전송**, **네트워크 안정성**, **CORS 정책** 등이 계층별로 얽혀 있다.

OSI 계층	관련 이슈	분석 포인트
7	HTTP PUT 요청 (파일 전송) / 403 오류	Presigned URL 유효시간 만료, 권한 문제
6	파일 MIME 타입(Content-Type) 변환	Content-Type: multipart/form-data 또는 image/png 확인
4	대용량 전송 시 TCP 세그먼트 단편화, 재전송	업로드 도중 속도 급감 시 전송계층 혼잡 제어 영향
3	외부 AWS S3 도메인으로 라우팅	DNS → Amazon Edge Node 확인
1~2	Wi-Fi 불안정 시 업로드 실패	실제 무선 간섭, 재전송 발생

→ **실무 팁:**

- Network 탭에서 "Failed to load resource" 발생 시 TCP 전송 실패 또는 네트워크 타임아웃일 가능성 높음.
- Presigned URL 생성 서버(NestJS)와 클라이언트 업로드 요청의 CORS 정책을 반드시 일치시켜야 함.

13-8-4. STT·AI 분석 API 호출 사례

상황:
"교권 보호용 음성 분석 시스템" 개발 중, 업로드된 음성 파일을 STT 엔진(Naver Clova)에 전송하여 결과(JSON)를 받아오는 과정에서 요청·응답 흐름을 분석.

OSI 계층	역할 및 구성 요소	설명
7	HTTP POST 요청 (/recog/v1/stt)	NCP OpenAPI 호출, Request Body: audio binary
6	Base64 인코딩, JSON 응답 파싱	응답 "text":"..." 데이터 처리
5	Access Key / Secret Key 인증 유지	X-NCP-APIGW-SIGNATURE-V2 헤더 포함
4	HTTPS(TCP 443) 안정적 전송	오디오 데이터 크기에 따라 TCP 세그먼트 분할
3	NCP 엔드포인트로 라우팅 (naveropenapi.apigw.ntruss.com)	DNS 조회 후 IP 연결
1~2	NIC → 라우터 → 인터넷 회선	내부망 방화벽, 프록시 설정 영향 가능

→ 분석 포인트:

- 응답이 늦을 경우 TTFB 증가 → 네트워크 혼잡 or STT API 응답지연.
- Access Key 오류 → 응용계층 인증 실패.
- JSON 파싱 실패 → 표현계층 데이터 포맷 오류.

13-8-5. 프론트엔드 성능 최적화와 네트워크 계층 활용

문제 유형	OSI 계층 관점 접근법	개선 방법
이미지/JS 파일 로딩 느림	7	CDN 사용, HTTP/2 적용, GZIP 압축
다수 API 동시 요청	7	HTTP/2 multiplexing 또는 GraphQL batching
TLS 연결 지연	6	TLS 세션 재사용, HTTP/3(QUIC) 적용
TCP 연결 재활용 안됨	4	Keep-Alive 유지, Connection Pool 적용
DNS 지연	3	DNS Prefetch, 캐시 TTL 최적화
Wi-Fi 불안정	1~2	유선 전환, NIC 드라이버 업데이트

13-8-6. 종합 정리

- 크롬 Network 탭은 단순 디버깅 도구가 아니라 **OSI 계층별 현상을 직관적으로 관찰할 수 있는 실무 플랫폼**이다.
- 웹 개발자는 코드 문제뿐 아니라 **전송 경로 전반의 병목**을 계층적으로 구분할 수 있어야 한다.
- 실제 업무에서는 다음 순서로 문제를 추적한다.
  ① 응용계층(API 요청/응답) → ② 전송계층(TCP 연결) → ③ 네트워크계층(DNS/IP) → ④ 물리계층(연결 품질).
- 이 구조를 이해하면, 단순 오류 확인을 넘어 **성능 튜닝·보안 강화·트러블슈팅 속도**까지 크게 향상된다.

14. 보안 관점에서 본 OSI 7계층의 이해와 적용

14-1. 개요

OSI 7계층은 단순히 데이터 통신의 구조를 설명하는 모델이 아니라, **각 계층별로 발생 가능한 위협(Threat)** 을 식별하고, 이에 대응하는 **보안 기술(Security Control)** 을 배치하기 위한 개념적 지도 역할을 합니다.

14-2. 계층별 주요 보안 위협 및 대응 기술

OSI 계층	주요 위협(공격 유형)	대표 보안 기술 / 대응 방법
7	SQL Injection, XSS, CSRF, 세션 하이재킹	WAF(Web Application Firewall), 입력값 검증, 토큰 인증, 보안 코딩, OWASP Top 10, API Security Top 10
6	암호화 미흡, 취약한 SSL/TLS 버전, 중간자 공격(MITM)	HTTPS(TLS 1.2+), 인증서 검증, HSTS, 암호 스위트 관리
5	세션 탈취, 세션 고정(Session Fixation)	세션 토큰 재발급, Secure 쿠키, 세션 타임아웃, MFA
4	포트 스캔, TCP 세션 하이재킹, SYN Flood (DoS)	방화벽(FW) 포트 제어, IDS/IPS, TCP SYN Cookie
3	IP 스푸핑, 라우팅 공격, DDoS, Ping Flood	ACL, 라우터 필터링, VPN, IPSec, Anti-DDoS, Zero Trust, ZTNA 개념(클라우드 보안 아키텍처)
2	ARP 스푸핑, MAC Flooding	스위치 포트보안, DAI(Dynamic ARP Inspection), VLAN 분리

1	케이블 절단, 비인가 단자 접속, 전자파 도청	출입통제, 케이블 관리, TEMPEST 차폐, 장비 격리, USB 데이터 차단, PoE 장비 보안(전력+데이터 혼용)

14-3. "보안은 계층적으로 쌓인다"는 의미

보안은 단일 장비로 완성되지 않습니다.
각 계층별로 역할이 다르기 때문에 **'Defense in Depth (다계층 방어)'** 개념이 중요합니다.

예시:

- **1~3계층:** 방화벽, IPS, VLAN, VPN
- **4~6계층:** TLS, IDS, IPSec
- **7계층:** WAF, 인증/인가, 로그 모니터링
- **보안 아키텍처:** L7 WAF → L4 FW → L3 Router ACL → L2 DAI → L1 물리보안

따라서 OSI 모델을 기반으로 **보안 솔루션의 배치 위치를 직관적으로 이해**할 수 있습니다.

14-4. 웹 서비스에서의 OSI 보안 계층 적용 예시

보안 위치	관련 OSI 계층	적용 기술 / 장비 예시
사용자와 서버 간 전송 보호	6~7	HTTPS, TLS 인증서, HSTS
API 서버 접근 제어	7	JWT, OAuth2, API Gateway, WAF
서버 간 내부 통신 보호	3~4	VPN, IPSec, 방화벽
네트워크 구간 분리	2~3	VLAN, L3 스위치, ACL 정책
물리적 접근 통제	1	출입통제 시스템, 네트워크 단자 차단장치

14-5. 사례: 실제 침해사고 분석 시 계층별 원인 구분

공격 사례	발생 OSI 계층	분석 결과	대응 조치
SQL Injection으로 DB 유출	7	입력값 필터링 미흡	보안코딩, ORM 사용, WAF 규칙 추가
SSL 인증서 만료로 접속 불가	6	TLS 인증 실패	인증서 자동갱신(Let's Encrypt 등)
포트 스캔 탐지	4	비인가 접근 탐색	방화벽 포트 제한, IDS 탐

			지
ARP 스푸핑으로 트래픽 탈취	2	로컬 스위치 공격	DAI, DHCP Snooping 활성화
공유기 해킹으로 패킷 변조	3	라우터 설정 취약	관리자 암호 변경, 펌웨어 업데이트
케이블 교체 시 외부 노출	1	물리적 보안 미흡	장비실 출입제어 강화

14-6. 개발자에게 필요한 보안 계층 이해 포인트

관점	주요 이해 포인트
프론트엔드 개발자	HTTPS 통신, 쿠키 보안 속성(SameSite, Secure), CSP(Content Security Policy)
백엔드 개발자	세션 관리, 인증/인가 구조(JWT, OAuth2), 입력값 검증, TLS 구성
인프라/보안 담당자	방화벽 정책, IDS/IPS 로그, VLAN 분리, 서버 접근 제어
R&D / AI 시스템 개발자	외부 API 호출 시 인증키 보호, STT 서버 통신 시 HTTPS 적용, Presigned URL 보안 만료시간 설정

14-7. 결론

- OSI 7계층은 **"데이터가 어떻게 이동하는가"**를 넘어서, **"공격이 어디서 발생할 수 있는가"**를 분석하기 위한 보안 프레임워크입니다.
- 따라서 개발·운영·보안을 통합적으로 이해하려면, 단순 통신 구조가 아닌 **계층별 위협 모델링(Threat Modeling)** 이 필수입니다.
- 특히 **웹서비스 보안 점검·침투테스트·망분리 설계** 시, OSI 모델을 기반으로 계층별 위험요소를 분리하면 훨씬 명확한 대응책을 수립할 수 있습니다.

14-8. 개발 실무자를 위한 필수 OSI 7계층 이해 포인트

14-8-1. 왜 개발자도 OSI 7계층을 알아야 하는가?

- 단순히 "코드"만 다루는 시대는 지났습니다.
  애플리케이션은 **네트워크, 보안, 클라우드 인프라**와 밀접하게 연결되어 있으며, 성능·보안·장애 대응에서 **계층적 이해가 곧 문제 해결력**으로 이어집니다.

- 개발자는 네트워크 엔지니어처럼 장비를 다루지 않더라도, "이 현상이 어느 계층에서 발생한 것인지"를 구분할 수 있어야 문제 원인을 정확히 찾아낼 수 있습니다.

14-8-2. 실무자가 반드시 이해해야 할 핵심 계층별 포인트

OSI 계층	개발 실무에서 반드시 알아야 할 포인트	이유 / 실제 사례
7	HTTP/HTTPS, REST, gRPC, WebSocket, GraphQL, JSON, MIME-Type	API 통신 구조, CORS 정책, Content-Type 불일치 문제 해결
6	데이터 인코딩(Base64, UTF-8), 암호화(TLS), 압축(GZIP)	TLS 인증서 문제, 응답이 깨짐(한글 인코딩 오류) 원인 파악
5	쿠키·세션·JWT·OAuth2 등 인증 방식	로그인 유지 실패, 세션 만료, 토큰 재발급 문제 해결
4	TCP/UDP 포트 개념, 3-Way Handshake, Keep-Alive	API 응답 지연 시 TCP 재전송·혼잡 제어 영향 분석
3	IP 주소, DNS, NAT, VPN, 라우팅 개념	서버 간 통신 차단, DNS 오류, 외부망 접근 불가 문제 대응
2	MAC 주소, VLAN, DHCP	사내망 통신 안됨, IP 충돌, VLAN 분리 환경에서 접근 문제
1	NIC, Wi-Fi, 케이블, 속도(Full/Half Duplex)	실제 연결 품질·대역폭 문제 분석 (ping, traceroute, iperf 등)

14-8-3. 개발자가 알아두면 큰 도움이 되는 실무 예시

상황	발생 OSI 계층	실무 팁
로컬 개발 환경에서 API 호출 시 CORS 오류 발생	7	브라우저 정책 기반(응용 계층 문제) → 서버 응답 헤더 수정
HTTPS 인증서 오류 (ERR_CERT_DATE_INVALID)	6	TLS 만료, 인증서 경로 문제 → 인증서 갱신/체인 점검
로그인 후 API 호출 시 401 Unauthorized	5	세션/토큰 누락 → JWT 또는 쿠키 갱신 로직 점검
백엔드 서버 응답 속도 느림	4	TCP 재전송, MTU 불일치 가능성 →

		Wireshark로 RTT 확인
DNS가 외부 IP로 잘못 해석됨	3	/etc/hosts 또는 DNS 캐시 문제 → DNS flush 또는 Resolver 변경
사내망에서는 정상, 외부망은 차단	3~4	방화벽 또는 VPN 정책 → 포트 허용 /ACL 확인
개발서버 ping 불가	1~3	NIC 불량, 스위치 포트 비활성화, VLAN 오설정 가능성

14-8-4. 클라우드 / AI / API 환경에서의 응용 예시

분야	필수 OSI 계층 이해 포인트	실제 문제 유형 / 체크포인트
클라우드 (AWS, NCP, GCP)	3~4	보안그룹(SG), VPC 서브넷, 포트 개방, NAT Gateway 설정
AI API (STT, GPT, Vision 등)	4~7	HTTPS 인증, JSON 응답 파싱, 요청 시간초과(TCP 지연)
모바일 앱 백엔드	3~7	DNS, API 라우팅, HTTPS 인증서, 세션 토큰 만료
CI/CD 서버 통신	3~4	GitHub Actions → 내부 서버 접근 시 VPN, 방화벽 규칙
IoT / RTSP 스트리밍	4 (UDP), 5	지연 최소화(UDP), 세션 유지, NAT Traversal 이해 필요

14-8-5. 개발자가 OSI 7계층을 실무에 적용하는 사고 흐름

문제 해결 단계 예시:

1) 증상 파악: "요청은 보냈는데 응답이 없다."

2) 계층 추적:

- 응용: 요청 URL, 포트, 헤더 확인.
- 전송: TCP 연결 여부(netstat, telnet, curl -v).
- 네트워크: ping/traceroute.
- 물리: 연결/Wi-Fi 신호 확인.

3) 원인 좁히기: 특정 계층에서만 실패하는지 구분.

4) 조치: 해당 계층별 설정 또는 코드 수정.

이 과정을 익히면 "이 문제는 어느 계층의 이슈인지" 빠르게 판별할 수 있습니다.

14-8-6. 실무자가 반드시 숙지해야 할 명령어 / 도구

도구/명령어	OSI 계층	용도 / 설명
ping, traceroute, pathping	3	IP 경로, 라우팅 확인
arp -a, ipconfig /all, ifconfig	1~2	NIC 정보, MAC 주소, IP 확인
netstat, ss, telnet, curl -v	4~7	포트 연결, TCP 세션, HTTP 헤더 확인
Wireshark, **Fiddler**, **Postman**	4~7	패킷 분석, HTTP 요청 검증, API 테스트
nslookup, **dig**	3	DNS 레코드 확인
openssl s_client -connect	6	TLS 인증서 유효성 검증
Chrome DevTools Network 탭	5~7	웹 요청·응답 구조 분석

14-8-7. 결론

- 개발자가 모든 계층을 깊게 파지 않아도 되지만, 최소한 **"증상이 발생했을 때 어느 계층의 문제인지 식별할 수 있는 수준"**은 필수입니다.
- 이러한 감각은 장애 대응, 성능 튜닝, 보안 강화에 모두 직결되며, **DevOps·Full-Stack·AI 서비스 개발자**라면 OSI 7계층은 **시스템 전체를 바라보는 사고 프레임워크**로써 반드시 익혀야 합니다.

부록 A. 약어(Abbreviations) 정리표

약어	영문명 (Full Name)	한글명	설명
ACL	Access Control List	접근 제어 목록	패킷의 출발지/목적지·포트·프로토콜 조건으로 허용/차단을 정의하는 정책 집합.
API	Application Programming Interface	응용 프로그램 인터페이스	소프트웨어 간 통신 규약 및 인터페이스.
ARP	Address Resolution Protocol	주소 결정 프로토콜	IP 주소를 MAC 주소로 변환하는 프로토콜.
BGP	Border Gateway Protocol	경계 게이트웨이 프로토콜	자율 시스템 간 라우팅 프로토콜 (인터넷 백본용).
CDN	Content Delivery Network	콘텐츠 전송 네트워크	사용자 근처 서버에서 콘텐츠를 빠르게 제공.
CLI	Command Line Interface	명령행 인터페이스	명령어 기반 시스템 제어 방식.
CoAP	Constrained Application Protocol	제약 환경용 응용 프로토콜	UDP 기반의 경량 REST 유사 프로토콜. 저전력/저용량 IoT 환경에 적합.
CORS	Cross-Origin Resource Sharing	교차 출처 리소스 공유	브라우저의 도메인 간 접근 제한 정책.
DAI	Dynamic ARP Inspection	동적 ARP 검사	ARP 위조 방지 스위치 보안 기능.
DHCP	Dynamic Host Configuration Protocol	동적 호스트 구성 프로토콜	자동으로 IP 주소를 할당하는 프로토콜.
DNS	Domain Name System	도메인 이름 시스템	도메인 이름을 IP 주소로 변환하는 시스템.
DNSSEC	Domain Name System Security Extensions	DNS 보안 확장	DNS 위·변조 방지를 위한 서명 기술.
FTP	File Transfer Protocol	파일 전송 프로토콜	파일 송수신용 응용계층 프로토콜.
GUI	Graphical User Interface	그래픽 사용자 인터페이스	시각적 인터페이스 기반의 조작 환경.
HTTP	HyperText Transfer Protocol	하이퍼텍스트 전송 프로토콜	웹 통신의 기본 프로토콜.
HTTPS	HyperText Transfer Protocol Secure	보안 하이퍼텍스트 전송 프로토콜	HTTP에 TLS 암호화를 적용한 안전한 통신 방식.

ICMP	Internet Control Message Protocol	인터넷 제어 메시지 프로토콜	네트워크 진단용(핑, 에러 보고 등) 프로토콜.
IDS/IPS	Intrusion Detection/Prevention System	침입 탐지/차단 시스템	비정상 트래픽 탐지 및 차단 보안 장비.
IMAP	Internet Message Access Protocol	인터넷 메시지 접근 프로토콜	이메일 수신·동기화용 프로토콜.
IP	Internet Protocol	인터넷 프로토콜	네트워크 간 패킷 전달(3계층 라우팅)의 기본 프로토콜.
JWT	JSON Web Token	제이슨 웹 토큰	인증·인가를 위한 토큰 기반 인증 구조.
LAN	Local Area Network	근거리 통신망	동일 지역(사무실 등) 내 네트워크.
MAC	Media Access Control	매체 접근 제어	네트워크 카드의 고유 하드웨어 주소(2계층 식별자).
MFA	Multi-Factor Authentication	다중 요소 인증	비밀번호 외에 OTP/지문/보안키 등 2개 이상의 인증 요소로 신원 확인.
MQTT	Message Queuing Telemetry Transport	경량 텔레메트리 메시징 프로토콜	TCP 기반 퍼블리시/구독 모델. IoT 센서·디바이스에 최적화(1883, TLS 8883).
MTU	Maximum Transmission Unit	최대 전송 단위	한 프레임에서 전송 가능한 최대 바이트 크기.
NAT	Network Address Translation	네트워크 주소 변환	내부 사설 IP를 공인 IP로 변환 (라우터 기능).
NIC	Network Interface Card	네트워크 인터페이스 카드	물리적 네트워크 연결 장치 (LAN 카드).
OSPF	Open Shortest Path First	최단 경로 우선 프로토콜	내부 라우팅 프로토콜 (링크 상태 기반).
PDU	Protocol Data Unit	프로토콜 데이터 단위	각 계층에서 사용하는 데이터 단위 (세그먼트·패킷·프레임 등).
QoE	Quality of Experience	사용자 체감 품질	네트워크 성능의 사용자 경험 지표.
QoS	Quality of Service	서비스 품질	네트워크 트래픽 우선순위 제어.
RTT	Round Trip Time	왕복 지연 시간	패킷이 목적지까지 갔다가 돌아오는 데 걸리는 시간.
SMTP	Simple Mail Transfer Protocol	간이 메일 전송 프로토콜	이메일 송신용 프로토콜.
SSL	Secure Sockets Layer	보안 소켓 계층	TLS의 이전 버전 (현재는 사용 권장 안

			함).
TCP	Transmission Control Protocol	전송 제어 프로토콜	신뢰성 있는 연결형 데이터 전송 (4계층).
TLS	Transport Layer Security	전송 계층 보안	HTTPS 등 암호화 통신을 위한 표준 보안 프로토콜.
TTFB	Time To First Byte	최초 바이트 수신 시간	서버 응답의 첫 바이트를 받는 데 걸리는 시간.
UDP	User Datagram Protocol	사용자 데이터그램 프로토콜	비연결형, 빠른 전송용 프로토콜 (4계층).
VLAN	Virtual Local Area Network	가상 랜	하나의 스위치를 논리적으로 여러 네트워크로 분리하는 기술.
VPN	Virtual Private Network	가상 사설망	암호화된 터널링으로 외부망 안전 연결.
WAF	Web Application Firewall	웹 애플리케이션 방화벽	응용계층 공격(XSS, SQLi 등) 방어.
WAN	Wide Area Network	광역 통신망	지리적으로 떨어진 네트워크 간 연결.
ZTNA	Zero Trust Network Access	제로 트러스트 네트워크 접근	"기본 불신" 원칙에 따라 사용자·디바이스·세션 맥락을 지속 검증하는 접근 제어 모델.

부록 B. 기술 용어 정리 (Glossary of Technical Terms)

용어	한글명	설명	관련 계층 / 영역
ARP	주소 결정 프로토콜	IP 주소를 MAC 주소로 변환 (IP→MAC 매핑).	2계층
Bandwidth	대역폭	네트워크가 단위 시간당 전송할 수 있는 데이터의 최대량.	1~2계층
CDN	콘텐츠 전송 네트워크	사용자 가까운 서버에서 정적 콘텐츠 제공.	응용계층
Chrome DevTools	크롬 개발자 도구	웹 요청·응답, 성능 TTFB, TLS 상태를 확인하는 브라우저 도구.	5~7계층
Connection Pool	연결 풀	다수의 백엔드 요청을 위해 미리 맺은 TCP/HTTP(S) 연결을 풀로 보관·재사용.	전송·응용
CORS	교차 출처 리소스 공유	브라우저의 도메인 간 요청 제한 정책 및 허용 규칙.	7계층 (웹)
Decapsulation	역캡슐화	수신 측에서 각 계층의 헤더를 벗겨 원본 데이터를 복원하는 과정.	전체 계층
DNS	도메인 이름 시스템	사람이 읽는 도메인을 IP 주소로 변환하는 시스템.	7→3계층
Duplex	듀플렉스	송수신 방식. Half = 교대로, Full = 동시 송수신.	1~2계층
Encapsulation	캡슐화	상위 계층 데이터에 하위 계층 헤더를 덧붙여 전송 단위(PDU)를 만드는 과정.	전체 계층
Firewall (FW)	방화벽	포트·프로토콜 기준으로 트래픽을 허용/차단하는 장비.	3~4계층
Frame	프레임	데이터링크 계층에서 사용하는 전송 단위 (MAC 주소 포함).	2계층
Handshake	핸드셰이크	연결 수립·보안 협상을 위한 절차 (예: TCP 3-Way, TLS Handshake).	전송·표현
Header	헤더	각 계층에서 데이터에 추가되는 제어 정보 (주소, 포트, 길이 등).	전 계층
HOLB (Head-of-Line Blocking)	헤드 오브 라인 블로킹	손실/지연된 선두 데이터가 뒤따르는 데이터까지 지연시키는 현상.	전송·응용
HSTS (HTTP Strict	HSTS(엄격 전송	브라우저에 HTTPS 전용 접근을 강제하는	응용·표현(보

Transport Security)	보안)	보안 정책.	안)
ICMP	인터넷 제어 메시지	네트워크 진단용 메시지 전송 프로토콜 (ping).	3계층
IDS/IPS	침입 탐지/차단 시스템	비정상 트래픽을 감시·차단하는 보안 장비.	3~4계층
JWT	JSON 웹 토큰	인증/인가를 위한 서명된 토큰 구조.	5~7계층
Keep-Alive	지속 연결	기존 TCP 연결을 재사용해 지연·오버헤드 감소.	전송·응용
Latency	지연 시간	데이터가 전송되어 응답이 돌아오기까지의 시간.	3~4계층
Load Balancer	부하 분산기	여러 서버로 트래픽을 분산 처리.	4 또는 7계층
mTLS (Mutual TLS)	상호 TLS	클라이언트·서버 양방향 인증.	표현(보안)·응용
MTU (Maximum Transmission Unit)	최대 전송 단위	한 프레임 또는 패킷의 최대 크기.	2~3계층
NAT (Network Address Translation)	네트워크 주소 변환	사설 IP를 공인 IP로 변환.	3계층
NAT Traversal	NAT 트래버설	NAT 환경에서 P2P 통신을 가능하게 하는 기법 (STUN/TURN/ICE).	네트워크·전송
OAuth2	인증 프로토콜	외부 서비스 인증용 표준 (구글/네이버 로그인 등).	5~7계층
Packet	패킷	네트워크 계층의 데이터 단위.	3계층
Payload	페이로드	상위 계층의 실제 데이터 내용 (헤더 제외).	전 계층
Ping	핑 테스트	ICMP Echo 기반 네트워크 연결성 테스트.	3계층
Port Number	포트 번호	애플리케이션을 구분하는 전송계층 논리 식별자.	4계층
Proxy Server	프록시 서버	클라이언트·서버 사이 중계, 캐싱, 보안 기능 제공.	7계층
PDU (Protocol Data Unit)	프로토콜 데이터 단위	계층별 데이터 단위 (세그먼트·패킷·프레임 등).	전 계층
QUIC	퀵	UDP 기반, TLS 내장 전송 프로토콜 (HTTP/3 기반).	전송·표현·응용

QoS (Quality of Service)	서비스 품질	트래픽 우선순위 및 대역폭 제어 기술.	2~3계층
Refresh Token	리프레시 토큰	액세스 토큰 만료 후 재발급용 장기 토큰.	세션·응용
Routing	라우팅	목적지까지의 최적 경로를 결정하는 과정.	3계층
Segment	세그먼트	전송계층 데이터 단위 (TCP/UDP 헤더 포함).	4계층
Session	세션	두 장치 간 논리적 연결 상태.	5계층
Snooping	스누핑	네트워크 트래픽을 감시·분석하는 행위.	2~3계층 (보안)
Socket	소켓	IP 주소 + 포트 번호로 구성된 통신 엔드포인트.	4~7계층
Throughput	처리량	실제 전송된 데이터의 양 (성능 지표).	3~4계층
TLS Handshake	TLS 핸드셰이크	HTTPS 통신 시 암호화 키 교환 및 인증 절차.	6계층
Traceroute	경로 추적	목적지까지의 라우터 경로 확인.	3계층
Wireshark	와이어샤크	네트워크 패킷 캡처·분석 도구.	2~7계층
WAF	웹 애플리케이션 방화벽	응용계층 공격(SQLi, XSS 등) 탐지 및 차단.	7계층